

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-142398
(P2001-142398A)

(43) 公開日 平成13年5月25日 (2001.5.25)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-ト* (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 Z 6 4 0 B

審査請求 未請求 請求項の数37 O L (全 20 頁)

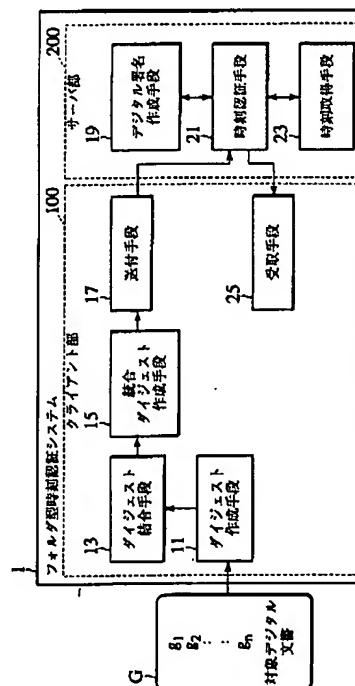
(21) 出願番号	特願2000-266194 (P2000-266194)	(71) 出願人	000004226 日本電信電話株式会社 東京都千代田区大手町二丁目3番1号
(22) 出願日	平成12年9月1日 (2000.9.1)	(72) 発明者	田倉 昭 東京都千代田区大手町二丁目3番1号 日 本電信電話株式会社内
(31) 優先権主張番号	特願平11-247993	(72) 発明者	小野 諭 東京都千代田区大手町二丁目3番1号 日 本電信電話株式会社内
(32) 優先日	平成11年9月1日 (1999.9.1)	(74) 代理人	100083806 弁理士 三好 秀和 (外1名)
(33) 優先権主張国	日本 (J P)		
(31) 優先権主張番号	特願平11-247994		
(32) 優先日	平成11年9月1日 (1999.9.1)		
(33) 優先権主張国	日本 (J P)		

(54) 【発明の名称】 フォルダ型時刻認証システムおよび分散時刻認証システム

(57) 【要約】

【課題】 パソコン上のデジタル文書を日常的に履歴の残る記録とし、かつ変更作成記録を第三者に証明することが可能となる時刻認証システムを提供すること。

【解決手段】 時刻認証システムにおいて、クライアント装置は、複数のデジタル文書に対する複数のダイジェストを作成し、作成された複数のダイジェストを結合し、結合された複数のダイジェストから統合ダイジェストを作成し、作成された統合ダイジェストを含んだ時刻認証要求をサーバ装置に送付して、サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取る。サーバ装置は、時刻認証要求に応じて取得された時刻情報と統合ダイジェストを結合して求められた時刻印付きデジタル文書と、時刻印付きデジタル文書に対するデジタル署名とを含んだ時刻認証証明書を作成する。



Best Available Copy

【特許請求の範囲】

【請求項1】 クライアント装置とサーバ装置からなる時刻認証システムであって、クライアント装置は、複数のデジタル文書に対する複数のダイジェストを作成するダイジェスト作成手段と、

このダイジェスト作成手段により作成された複数のダイジェストを結合するダイジェスト結合手段と、

このダイジェスト結合手段により結合された複数のダイジェストから統合ダイジェストを作成する統合ダイジェスト作成手段と、

この統合ダイジェスト作成手段により作成された統合ダイジェストを含んだ時刻認証要求をサーバ装置に送付する送付手段と、

サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取る受取手段とを有し、

サーバ装置は、時刻認証要求に応じて取得された時刻情報と統合ダイジェストを結合して求められた時刻印付きデジタル文書と、時刻印付きデジタル文書に対するデジタル署名とを含んだ時刻認証証明書を作成することを特徴とする時刻認証システム。

【請求項2】 クライアント装置は更に、パソコンまたはネットワーク上のデジタル文書から前記複数のデジタル文書を、ファイルまたはフォルダ単位で指定するデジタル文書指定手段を有することを特徴とする請求項1記載の時刻認証システム。

【請求項3】 デジタル文書指定手段は、前記複数のデジタル文書に以前に取得した時刻認証証明書が含まれるように、前記複数のデジタル文書を指定することを特徴とする請求項2記載の時刻認証システム。

【請求項4】 クライアント装置は更に、ダイジェスト作成手段に定期的なダイジェスト作成時刻を指定して、ダイジェスト作成手段がこの定期的なダイジェスト作成時刻に前記複数のダイジェストを定期的に作成するようにする時刻指定手段を有することを特徴とする請求項1記載の時刻認証システム。

【請求項5】 クライアント装置は更に、受取手段で受け取った時刻認証証明書に含まれるデジタル署名が正しいか否か検証する検証手段を有することを特徴とする請求項1記載の時刻認証システム。

【請求項6】 クライアント装置は更に、受取手段で受け取った時刻認証証明書に含まれる時刻印付きデジタル文書によって示される時刻が、送付手段における時刻認証要求の送付時刻と、受取手段における時刻認証証明書の受取時刻の間にあることを検証する検証手段を有することを特徴とする請求項1記載の時刻認証システム。

【請求項7】 サーバ装置は、統合ダイジェストと時刻情報を結合して時刻印付きデジタル文書を求め、時刻印付きデジタル文書に対するデジタル署名を生成するデジタル署名手段と、このデジタル署名手段により生成された時刻印付きデジ

タル文書とデジタル署名から時刻認証証明書を作成する時刻認証証明書作成手段と、

を有することを特徴とする請求項1記載の時刻認証システム。

【請求項8】 サーバ装置は、

複数の時刻取得手段で、各時刻取得手段は、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻情報を順次取得する時刻取得手段と、

これら複数の時刻取得手段に対応して設けられた複数の結合手段で、各結合手段は、他の結合手段とは独立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成する結合手段と、

これら複数の結合手段に対応して設けられた複数のデジタル署名手段で、各デジタル署名手段は、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するデジタル署名手段と、

複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成する統合デジタル署名作成手段と、

この統合デジタル署名作成手段により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成する時刻認証証明書作成手段と、

を有することを特徴とする請求項1記載の時刻認証システム。

【請求項9】 各デジタル署名手段は、前記同一時刻になる可能性のない時刻の時刻印付きデジタル文書の少なくとも一つに対するデジタル署名を生成しないように制御されることを特徴とする請求項8記載の時刻認証システム。

【請求項10】 統合デジタル署名作成手段と時刻認証証明書作成手段が時刻認証機関を構成し、時刻取得手段と結合手段とデジタル署名手段の各組が分散部分時刻認証機関を構成することを特徴とする請求項8記載の時刻認証システム。

【請求項11】 複数のデジタル文書に対する複数のダイジェストを作成するダイジェスト作成手段と、

このダイジェスト作成手段により作成された複数のダイジェストを結合するダイジェスト結合手段と、

このダイジェスト結合手段により結合された複数のダイジェストから統合ダイジェストを作成する統合ダイジェスト作成手段と、

この統合ダイジェスト作成手段により作成された統合ダイジェストを含んだ時刻認証要求を時刻認証システムの

サーバ装置に送付する送付手段と、
サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取る受取手段と、
を有することを特徴とする時刻認証システムのクライアント装置。

【請求項12】 パソコンまたはネットワーク上のデジタル文書から前記複数のデジタル文書を、ファイルまたはフォルダ単位で指定するデジタル文書指定手段を更に有することを特徴とする請求項1記載のクライアント装置。

【請求項13】 デジタル文書指定手段は、前記複数のデジタル文書に以前に取得した時刻認証証明書が含まれるように、前記複数のデジタル文書を指定することを特徴とする請求項12記載のクライアント装置。

【請求項14】 ダイジェスト作成手段に定期的なダイジェスト作成時刻を指定して、ダイジェスト作成手段がこの定期的なダイジェスト作成時刻に前記複数のダイジェストを定期的に作成するようにする時刻指定手段を更に有することを特徴とする請求項1記載のクライアント装置。

【請求項15】 受取手段で受け取った時刻認証証明書に含まれるデジタル署名が正しいか否か検証する検証手段を更に有することを特徴とする請求項1記載のクライアント装置。

【請求項16】 受取手段で受け取った時刻認証証明書に含まれる時刻印付きデジタル文書によって示される時刻が、送付手段における時刻認証要求の送付時刻と、受取手段における時刻認証証明書の受取時刻の間にあることを検証する検証手段を更に有することを特徴とする請求項1記載のクライアント装置。

【請求項17】 複数の時刻取得手段で、各時刻取得手段は、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻情報を順次取得する時刻取得手段と、
これら複数の時刻取得手段に対応して設けられた複数の結合手段で、各結合手段は、他の結合手段とは独立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成する結合手段と、
これら複数の結合手段に対応して設けられた複数のデジタル署名手段で、各デジタル署名手段は、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するデジタル署名手段と、
複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成する統合デジタル署名作成手段と、

この統合デジタル署名作成手段により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成する時刻認証証明書作成手段と、
を有することを特徴とする時刻認証システムのサーバ装置。

【請求項18】 各デジタル署名手段は、前記同一時刻になる可能性のない時刻の時刻印付きデジタル文書の少なくとも一つに対するデジタル署名を生成しないように制御されることを特徴とする請求項17記載のサーバ装置。

【請求項19】 統合デジタル署名作成手段と時刻認証証明書作成手段が時刻認証機関を構成し、時刻取得手段と結合手段とデジタル署名手段の各組が分散部分時刻認証機関を構成することを特徴とする請求項17記載のサーバ装置。

【請求項20】 クライアント装置とサーバ装置からなる時刻認証システムにおける時刻認証方法であって、
(a) クライアント装置において、複数のデジタル文書に対する複数のダイジェストを作成するステップと、
(b) クライアント装置において、ステップ(a)により作成された複数のダイジェストを結合するステップと、
(c) クライアント装置において、ステップ(b)により結合された複数のダイジェストから統合ダイジェストを作成するステップと、
(d) ステップ(c)により作成された統合ダイジェストを含んだ時刻認証要求をクライアント装置からサーバ装置に送付するステップと、
(e) サーバ装置において、時刻認証要求に応じて取得された時刻情報と統合ダイジェストを結合して求められた時刻印付きデジタル文書と、時刻印付きデジタル文書に対するデジタル署名とを含んだ時刻認証証明書を作成するステップと、
(f) クライアント装置において、サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取るステップと、
を有することを特徴とする時刻認証方法。

【請求項21】 クライアント装置において、パソコンまたはネットワーク上のデジタル文書から前記複数のデジタル文書を、ファイルまたはフォルダ単位で指定するステップを更に有することを特徴とする請求項20記載の時刻認証方法。

【請求項22】 前記指定するステップは、前記複数のデジタル文書に以前に取得した時刻認証証明書が含まれるように、前記複数のデジタル文書を指定することを特徴とする請求項21記載の時刻認証方法。

【請求項23】 クライアント装置において、定期的なダイジェスト作成時刻を指定して、ステップ(a)がこの定期的なダイジェスト作成時刻に前記複数のダイジェ

ストを定期的に変成するようにするステップを更に有することを特徴とする請求項20記載の時刻認証方法。

【請求項24】 クライアント装置において、ステップ(f)で受け取った時刻認証証明書に含まれるデジタル署名が正しいか否かを検証するステップを更に有することを特徴とする請求項20記載の時刻認証方法。

【請求項25】 クライアント装置において、ステップ(f)で受け取った時刻認証証明書に含まれる時刻印付きデジタル文書によって示される時刻が、ステップ(d)における時刻認証要求の送付時刻と、ステップ(f)における時刻認証証明書の受取時刻の間にあることを検証するステップを更に有することを特徴とする請求項20記載の時刻認証方法。

【請求項26】 前記ステップ(e)は、
(e1)サーバ装置の複数の時刻取得手段の各時刻取得手段において、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻情報を順次取得するステップと、

(e2)サーバ装置のこれら複数の時刻取得手段に対応して設けられた複数の結合手段の各結合手段において、他の結合手段とは独立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成するステップと、

(e3)サーバ装置のこれら複数の結合手段に対応して設けられた複数のデジタル署名手段の各デジタル署名手段において、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するステップと、

(e4)複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成するステップと、

(e5)ステップ(e4)により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成するステップと、
を有することを特徴とする請求項20記載の時刻認証方法。

【請求項27】 前記ステップ(e3)において、各デジタル署名手段は、前記同一時刻になる可能性のない時刻の時刻印付きデジタル文書の少なくとも一つに対するデジタル署名を生成しないように制御されることを特徴とする請求項26記載の時刻認証方法。

【請求項28】 時刻認証システムのクライアント装置において時刻認証サービスを受ける方法であって、

(a)複数のデジタル文書に対する複数のダイジェストを作成するステップと、

(b)ステップ(a)により作成された複数のダイジェ

ストを結合するステップと、

(c)ステップ(b)により結合された複数のダイジェストから統合ダイジェストを作成するステップと、

(d)ステップ(c)により作成された統合ダイジェストを含んだ時刻認証要求を時刻認証システムのサーバ装置に送付するステップと、

(e)サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取るステップと、

を有することを特徴とする時刻認証サービスを受ける方法。

【請求項29】 パソコンまたはネットワーク上のデジタル文書から前記複数のデジタル文書を、ファイルまたはフォルダ単位で指定するステップを更に有することを特徴とする請求項28記載の時刻認証サービスを受ける方法。

【請求項30】 前記指定するステップは、前記複数のデジタル文書に以前に取得した時刻認証証明書が含まれるように、前記複数のデジタル文書を指定することを特徴とする請求項29記載の時刻認証サービスを受ける方法。

【請求項31】 クライアント装置において、定期的なダイジェスト作成時刻を指定して、ステップ(a)がこの定期的なダイジェスト作成時刻に前記複数のダイジェストを定期的に変成するようにするステップを更に有することを特徴とする請求項28記載の時刻認証サービスを受ける方法。

【請求項32】 時刻認証証明書は、時刻認証要求に応じて取得された時刻情報と統合ダイジェストを結合して求められた時刻印付きデジタル文書と、時刻印付きデジタル文書に対するデジタル署名とを含んでおり、クライアント装置において、ステップ(e)で受け取った時刻認証証明書に含まれるデジタル署名が正しいか否かを検証するステップを更に有することを特徴とする請求項28記載の時刻認証サービスを受ける方法。

【請求項33】 時刻認証証明書は、時刻認証要求に応じて取得された時刻情報と統合ダイジェストを結合して求められた時刻印付きデジタル文書と、時刻印付きデジタル文書に対するデジタル署名とを含んでおり、クライアント装置において、ステップ(e)で受け取った時刻認証証明書に含まれる時刻印付きデジタル文書によって示される時刻が、ステップ(d)における時刻認証要求の送付時刻と、ステップ(e)における時刻認証証明書の受取時刻の間にあることを検証するステップを更に有することを特徴とする請求項28記載の時刻認証サービスを受ける方法。

【請求項34】 時刻認証システムのサーバ装置において時刻認証サービスを提供する方法であって、

(a)サーバ装置の複数の時刻取得手段の各時刻取得手段において、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻

情報を順次取得するステップと、

(b) サーバ装置のこれら複数の時刻取得手段に対応して設けられた複数の結合手段の各結合手段において、他の結合手段とは独立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成するステップと、

(c) サーバ装置のこれら複数の結合手段に対応して設けられた複数のデジタル署名手段の各デジタル署名手段において、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するステップと、

(d) 複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成するステップと、

(e) ステップ(d)により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成するステップと、
を有することを特徴とする時刻認証サービスを提供する方法。

【請求項35】 前記ステップ(c)において、各デジタル署名手段は、前記同一時刻になる可能性のない時刻の時刻印付きデジタル文書の少なくとも一つに対するデジタル署名を生成しないように制御されることを特徴とする請求項34記載の時刻認証サービスを提供する方法。

【請求項36】 コンピュータを時刻認証システムのクライアント装置として機能させるためのコンピュータ読み取り可能なプログラムコードを格納したコンピュータ利用可能な記録媒体であって、該コンピュータ読み取り可能なプログラムコードは、
複数のデジタル文書に対する複数のダイジェストを作成する第一のプログラムコードと、
この第一のプログラムコードにより作成された複数のダイジェストを結合する第二のプログラムコードと、
この第二のプログラムコードにより結合された複数のダイジェストから統合ダイジェストを作成する第三のプログラムコードと、
この第三のプログラムコードにより作成された統合ダイジェストを含んだ時刻認証要求を時刻認証システムのサーバ装置に送付する第四のプログラムコードと、
サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取る第五のプログラムコードと、
を有することを特徴とする記録媒体。

【請求項37】 少なくとも一つのコンピュータを時刻認証システムのサーバ装置として機能させるためのコンピュータ読み取り可能なプログラムコードを格納したコ

ンピュータ利用可能な記録媒体であって、該コンピュータ読み取り可能なプログラムコードは、

複数の時刻取得手段で、各時刻取得手段は、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻情報を順次取得する時刻取得手段を実現するための第一のプログラムコードと、
これら複数の時刻取得手段に対応して設けられた複数の結合手段で、各結合手段は、他の結合手段とは独立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成する結合手段を実現するための第二のプログラムコードと、

これら複数の結合手段に対応して設けられた複数のデジタル署名手段で、各デジタル署名手段は、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するデジタル署名手段を実現するための第三のプログラムコードと、

複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成する第四のプログラムコードと、

この統合デジタル署名作成手段により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成する第五のプログラムコードと、

を有することを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はデジタル文書に時刻印を押すサービスにおいて、デジタル文書が時刻印を押された時点以降において変更されてなく、かつ確かに時刻印が押された時点で対象とするデジタル文書が存在していたことを証明することを可能とするフォルダ型時刻認証システムおよび分散時刻認証システムに関する。

【0002】

【従来の技術】例えば米国における先発明主義に基づく特許制度の下では日付の入った研究ノートが優先権を証明する証拠として用いることが可能であり、さらに日付の付けられた家計簿は確定申告における支出記録として使うことができることが知られる。一方、パソコンが日常的に使用されるようになるにつれ、研究ノートや家計簿などの日常記録をパソコンを用いて行うことがごく一般的になってきている。

【0003】しかしながら、このようなパソコン上での電氣的、デジタル的な記録によるものは容易に書き換えることができることから、記録媒体としての紙を用いて書かれた記録とは異なり、記録日時を含め記録内容を第

三者に証明することができないという問題を有していた。

【0004】これに対し従来、デジタル文書に時刻印を押すサービスとして、特開平7-254897号公報に記載の「個人用日時認証装置」が知られる。この個人用日時認証装置は、スマートカード等に時刻認証装置を組み込み、デジタル署名を行うときに時刻認証と一緒に行うものである。また、特開平3-185551号公報に記載の「デジタル時間認証装置」は、時刻認証装置を一つのハードウェアプラットフォームとして作成し、文書の作成者がその装置を使って時刻認証を行うものである。これらはいずれも、文書作成者が時刻認証を行う方式であるため、偽造がしやすく、第三者機関による証明でないため信頼性が乏しいものとなっている。

【0005】また特開平6-14018号公報に記載の「電子的公証方法および装置」は、元の文書に対するCRC (Cyclic Redundancy Check ; 巡回冗長検査)、パリティ、検査合計を組み合わせて圧縮文書を作成し、時刻認証を行うものである。この方式で作成される圧縮文書は、現在広く暗号技術として使われているハッシュ関数(例えばMD5やSHA-1など)を用いて作成する圧縮文書と比較して同一の圧縮文書をもつデジタル文書の偽造がしやすい。

【0006】さらに特表平6-501571号公報に記載の「数値文書に確実にタイムスタンプを押す方法」は、時刻認証を行う外部機関が単独で時刻認証証明書を作成するものである。このタイムスタンプを押す方法は、外部機関が時刻認証証明書を偽造することが容易である。

【0007】この欠点を補うために、受け取った時刻認証要求とその外部機関が直前に発行した時刻認証証明書を結合したデジタル文書に対してハッシュ関数を適用して得られた圧縮文書にデジタル署名を行い時刻認証証明書を作成する方法が提案されている。この方法は、時刻認証外部機関が時刻認証証明書を偽造することを事実上不可能にしているが、異なるラウンド(複数の時刻認証証明書を発行する一定期間)内での順序が正しい順序であるかどうかを検証することはできない。

【0008】また、時刻認証証明書が真正であることを証明するためには、それ以前に発行した証明書が必要となる。すなわち、時刻認証外部機関が発行したすべての時刻認証証明書を保存するか、定期的に衆目にさらされたその時点での時刻認証証明書の値に辿り着くまでの時刻認証証明書を保存しておかないと、時刻認証証明書が真正であることを証明することができない。このため、システムとして膨大な記憶容量を必要とするとともに、真正であることの証明に膨大な時間を必要とする。

【0009】現在、IETF (Internet Engineering Task Force) においてハッシュ関数により圧縮されたデジタル文書を外部機関に送付し、送付された圧縮デジ

タル文書に対して時刻認証証明書を作成するプロトコルの標準化が進められている。ここで標準化が検討されている方式においては、外部機関は1ヶ所で時刻認証証明書を作成するため、時刻認証証明書の偽造の可能性および時刻認証証明書を取得することが許されていない悪意のある第三者が不正に時刻認証証明書を取得する危険性を排除することができないという問題点をすでに含んでいる。

【0010】

【発明が解決しようとする課題】一方、特願平11-35761号に記載の「時刻認証装置」では、時刻認証機関が単独でデジタル署名を作成するのではなく、公開鍵暗号における秘密鍵を分割したものに相当する部分秘密鍵を一つの時刻認証機関が所有し、第三者機関である各部分署名機関が独立に部分署名を作成することにより、時刻認証手段による時刻認証証明書の偽造を防止する手段を提供している。この時刻認証装置では、時刻認証手段を利用するクライアント側で、文書の作成履歴を定期的に作成し、その文書作成履歴に関する時刻認証証明書を時刻認証手段により作成することにより信頼性の高いデジタル文書の存在証明が可能となる。

【0011】また、サーバ側では、時刻認証を行う外部機関が一つの秘密鍵を用いてデジタル署名を行う場合における秘密鍵の盗難の危険性やデジタル文書の著作者と時刻認証外部機関が結託して過去にさかのぼった時刻印を押す偽造の危険性を排除するために、時刻認証装置の秘密鍵を複数のデジタル署名手段が分割して持ち、それぞれのデジタル署名手段が独立してデジタル署名を行う。これにより秘密鍵盗難の危険性をなくするとともに、時刻を取得する手段とデジタル署名を行う手段を実行するすべての機関が結託しない限り時刻印を偽造することができないようにすることにより安全で信頼のおける時刻認証サービスを行う時刻認証外部機関を運営することができる。また、過去に発行した時刻認証証明書を一切保管する必要はなく、上述したような従来手法と比較して大幅に記憶容量を削減することが可能である。

【0012】しかしながら、分散した時刻認証機関が部分秘密鍵を用いて同一のデジタル文書に時刻署名を独立に行う場合、全く同一の時刻を付けたデジタル文書にデジタル署名を行わないと、分散秘密鍵に対応する公開鍵でデジタル署名を検証することができない。

【0013】本発明は、上記課題に鑑みてなされたもので、例えばパソコン上のデジタル文書に対して定期的に信頼のおける第三者機関から存在証明のための時刻認証証明書を取得しておくことにより、パソコン上のデジタル文書を研究ノートや家計簿と同様な日常的に履歴の残る記録とし、しかもその変更作成記録を第三者に証明することが可能な記録媒体として活用することができるフォルダ型時刻認証システムを提供することを目的とする。

【0014】また、本発明は、独立に時刻署名を分散して行うときの複数の部分デジタル署名結果から得られる統合デジタル署名を一つの公開鍵を用いて復号し得るようにする分散時刻認証システムを提供することを目的とする。

【0015】

【課題を解決するための手段】上記課題を解決するために、本発明は、クライアント装置とサーバ装置からなる時刻認証システムであって、クライアント装置は、複数のデジタル文書に対する複数のダイジェストを作成するダイジェスト作成手段と、このダイジェスト作成手段により作成された複数のダイジェストを結合するダイジェスト結合手段と、このダイジェスト結合手段により結合された複数のダイジェストから統合ダイジェストを作成する統合ダイジェスト作成手段と、この統合ダイジェスト作成手段により作成された統合ダイジェストを含んだ時刻認証要求をサーバ装置に送付する送付手段と、サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取る受取手段とを有し、サーバ装置は、時刻認証要求に応じて取得された時刻情報と統合ダイジェストを結合して求められた時刻印付きデジタル文書と、時刻印付きデジタル文書に対するデジタル署名とを含んだ時刻認証証明書を生成することを特徴とする時刻認証システムを提供する。

【0016】また、本発明は、複数のデジタル文書に対する複数のダイジェストを作成するダイジェスト作成手段と、このダイジェスト作成手段により作成された複数のダイジェストを結合するダイジェスト結合手段と、このダイジェスト結合手段により結合された複数のダイジェストから統合ダイジェストを作成する統合ダイジェスト作成手段と、この統合ダイジェスト作成手段により作成された統合ダイジェストを含んだ時刻認証要求を時刻認証システムのサーバ装置に送付する送付手段と、サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取る受取手段と、を有することを特徴とする時刻認証システムのクライアント装置を提供する。

【0017】また、本発明は、複数の時刻取得手段で、各時刻取得手段は、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻情報を順次取得する時刻取得手段と、これら複数の時刻取得手段に対応して設けられた複数の結合手段で、各結合手段は、他の結合手段とは独立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成する結合手段と、これら複数の結合手段に対応して設けられた複数のデジタル署名手段で、各デジタル署名手段は、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するデジタル署名手段と、複数のデジタル署名手段によって生成さ

れた複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成する統合デジタル署名作成手段と、この統合デジタル署名作成手段により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成する時刻認証証明書作成手段と、を有することを特徴とする時刻認証システムのサーバ装置を提供する。

【0018】また、本発明は、クライアント装置とサーバ装置からなる時刻認証システムにおける時刻認証方法であって、(a)クライアント装置において、複数のデジタル文書に対する複数のダイジェストを作成するステップと、(b)クライアント装置において、ステップ(a)により作成された複数のダイジェストを結合するステップと、(c)クライアント装置において、ステップ(b)により結合された複数のダイジェストから統合ダイジェストを作成するステップと、(d)ステップ(c)により作成された統合ダイジェストを含んだ時刻認証要求をクライアント装置からサーバ装置に送付するステップと、(e)サーバ装置において、時刻認証要求に応じて取得された時刻情報と統合ダイジェストを結合して求められた時刻印付きデジタル文書と、時刻印付きデジタル文書に対するデジタル署名とを含んだ時刻認証証明書を生成するステップと、(f)クライアント装置において、サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取るステップと、を有することを特徴とする時刻認証方法を提供する。

【0019】また、本発明は、時刻認証システムのクライアント装置において時刻認証サービスを受ける方法であって、(a)複数のデジタル文書に対する複数のダイジェストを作成するステップと、(b)ステップ(a)により作成された複数のダイジェストを結合するステップと、(c)ステップ(b)により結合された複数のダイジェストから統合ダイジェストを作成するステップと、(d)ステップ(c)により作成された統合ダイジェストを含んだ時刻認証要求を時刻認証システムのサーバ装置に送付するステップと、(e)サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取るステップと、を有することを特徴とする時刻認証サービスを受ける方法を提供する。

【0020】また、本発明は、時刻認証システムのサーバ装置において時刻認証サービスを提供する方法であって、(a)サーバ装置の複数の時刻取得手段の各時刻取得手段において、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻情報を順次取得するステップと、(b)サーバ装置のこれら複数の時刻取得手段に対応して設けられた複数の結合手段の各結合手段において、他の結合手段とは独

立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成するステップと、

(c) サーバ装置のこれら複数の結合手段に対応して設けられた複数のデジタル署名手段の各デジタル署名手段において、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するステップと、(d) 複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成するステップと、(e) ステップ(d)により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成するステップと、を有することを特徴とする時刻認証サービスを提供する方法を提供する。

【0021】また、本発明は、コンピュータを時刻認証システムのクライアント装置として機能させるためのコンピュータ読み取り可能なプログラムコードを格納したコンピュータ利用可能な記録媒体であって、該コンピュータ読み取り可能なプログラムコードは、複数のデジタル文書に対する複数のダイジェストを作成する第一のプログラムコードと、この第一のプログラムコードにより作成された複数のダイジェストを結合する第二のプログラムコードと、この第二のプログラムコードにより結合された複数のダイジェストから統合ダイジェストを作成する第三のプログラムコードと、この第三のプログラムコードにより作成された統合ダイジェストを含んだ時刻認証要求を時刻認証システムのサーバ装置に送付する第四のプログラムコードと、サーバ装置から前記複数のデジタル文書に対する時刻認証証明書を受け取る第五のプログラムコードと、を有することを特徴とする記録媒体を提供する。

【0022】また、本発明は、少なくとも一つのコンピュータを時刻認証システムのサーバ装置として機能させるためのコンピュータ読み取り可能なプログラムコードを格納したコンピュータ利用可能な記録媒体であって、該コンピュータ読み取り可能なプログラムコードは、複数の時刻取得手段で、各時刻取得手段は、時刻認証要求に応じて、他の時刻取得手段とは独立に、所定の一定の刻み幅で与えられた前記時刻情報を順次取得する時刻取得手段を実現するための第一のプログラムコードと、これら複数の時刻取得手段に対応して設けられた複数の結合手段で、各結合手段は、他の結合手段とは独立に、対応する時刻取得手段により順次取得された時刻情報を統合ダイジェストを含んだデータを順次結合して複数の時刻印付きデジタル文書を作成する結合手段を実現するための第二のプログラムコードと、これら複数の結合手段

に対応して設けられた複数のデジタル署名手段で、各デジタル署名手段は、他のデジタル署名手段とは独立に、対応する結合手段により作成された各時刻印付きデジタル文書に対するデジタル署名を生成するデジタル署名手段を実現するための第三のプログラムコードと、複数のデジタル署名手段によって生成された複数のデジタル署名から、複数のデジタル署名手段によって同一時刻の時刻印付きデジタル文書に対して生成された複数のデジタル署名を、各デジタル署名手段毎に一つずつ選択し、選択されたデジタル署名から統合デジタル署名を作成する第四のプログラムコードと、この統合デジタル署名作成手段により作成された統合デジタル署名と前記同一時刻の時刻印付きデジタル文書から時刻認証証明書を作成する第五のプログラムコードと、を有することを特徴とする記録媒体を提供する。

【0023】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【0024】図1に本発明の第一の実施形態に係るフォルダ型時刻認証システムの構成を示す。

【0025】図1において、フォルダ型時刻認証システム1は、テキスト情報、画像情報、音声情報が適宜、含まれるデジタル文書の内、対象となる対象デジタル文書Gのダイジェストを作成するダイジェスト作成手段11と、このダイジェスト作成手段11で作成される複数のダイジェストを結合するダイジェスト結合手段13と、このダイジェスト結合手段13で複数のダイジェストを結合して得られた全体の結果に対して統合ダイジェストを作成する統合ダイジェスト作成手段15と、この統合ダイジェスト作成手段15で作成された統合ダイジェストを含むデータを時刻認証手段21を介してデジタル署名作成手段19に送付する送付手段17と、この送付手段17を介して前記統合ダイジェスト作成手段15から受け取った統合ダイジェストを含むデータに後述する時刻取得手段23から取得した時刻を結合し、この結合した全体に対してデジタル署名を作成するデジタル署名作成手段19と、これら各手段で作成され、取得された統合ダイジェスト、時刻、デジタル署名を含む時刻認証証明書を受取手段25に送付する時刻認証手段21と、この時刻認証手段21により問い合わせのあった時点の時刻を時刻情報として提供する時刻取得手段23と、前記時刻認証手段21から送られる時刻認証証明書を受け取る受取手段25により構成される。

【0026】ここで、ダイジェスト作成手段11と、ダイジェスト結合手段13と、統合ダイジェスト作成手段15と、送付手段17と、受取手段25がクライアント部100を構成し、デジタル署名作成手段19と時刻認証手段21と時刻取得手段23がサーバ部200を構成する。

【0027】以下、図1を参照して、第一の実施形態に

における時刻認証処理について説明する。

【0028】著作者により作成されたテキスト情報、画像情報、音声情報、バイナリ情報あるいはそれらの組み合わせからなる対象デジタル文書Gは、フォルダ型時刻認証システム1内のダイジェスト作成手段11により、処理の高速化を計るとともに、サーバ部200に元の文書を送付せずに済むようにし、しかも異なる文書に対して非常に高い確率で異なる値が得られるようにするために、各デジタル文書毎にハッシュ関数（例えばSHA-1やMD5）を用いてダイジェストが作成される。

【0029】具体的には、ハッシュ関数を h 、対象デジタル文書Gを構成する複数のデジタル文書 g_1, g_2, \dots, g_n とすると、ダイジェスト作成手段11によりダイジェスト $h(g_1), h(g_2), \dots, h(g_n)$ が作成される。

【0030】次に、ダイジェスト結合手段13により、例えば、各ダイジェスト $h(g_1), h(g_2), \dots, h(g_n)$ を接続により結合した結果として $h(g_1) \cdot h(g_2) \dots h(g_n)$ を得る。この結合結果から統合ダイジェスト作成手段15により統合ダイジェストを作成する。

【0031】ここで統合ダイジェスト作成手段15で用いるハッシュ関数を i とすると、 $i(h(g_1) \cdot h(g_2) \dots h(g_n))$ が統合ダイジェストとなる。統合ダイジェスト $i(h(g_1) \cdot h(g_2) \dots h(g_n))$ を送付手段17により時刻認証手段21を介してデジタル署名作成手段19に送付する。

【0032】デジタル署名作成手段19は、統合ダイジェスト $i(h(g_1) \cdot h(g_2) \dots h(g_n))$ と時刻取得手段23により取得した時刻 t を含むデジタルデータに対してデジタル署名 s を作成し、このデジタル署名 s を時刻認証手段21に送出する。

【0033】続いて、時刻認証手段21では、このデジタル署名 s と、統合ダイジェスト $i(h(g_1) \cdot h(g_2) \dots h(g_n))$ および時刻 t を含む時刻認証証明書を発行し受取手段25に送出する。

【0034】第一の実施形態によれば、パソコン上のデジタル文書に対して定期的に信頼のおける第三者機関に存在証明のための時刻認証証明書を発行してもらうことにより、関連する文書や図、表などが一体となって一つの体系的な文書を構成することが多いデジタル文書においても、パソコン上のデジタル文書を、それらの関連文書あるいはそれらを作成しているパソコン上にある他のデジタル文書と関連付けて、時刻認証証明書を取得しておくことが可能となる。

【0035】また、時刻認証を行った文書の存在証明の信頼性を向上することができ、さらにパソコン上のデジタル文書を研究ノートや家計簿と同様な日常的に履歴の残る記録とし、しかもその変更作成記録を第三者に証明することが可能な記録媒体として活用することができ

る。

【0036】これにより、複数のデジタル文書が時刻印を押された時点以降において変更されてなく、かつ確かに時刻印が押された時点でこれら複数のデジタル文書が同時に存在していたことを証明することが可能となる。しかも、各デジタル文書毎に時刻認証証明書の要否を判定する必要がなく、複数のデジタル文書に対してまとめて一つの時刻認証証明書を取得すればよくなるため、時刻認証サービスを低コストで活用することが可能となる。

【0037】次に、図2に本発明の第二の実施形態に係るフォルダ型時刻認証システムの構成を示す。

【0038】図2において、フォルダ型時刻認証システム3は、テキスト文書、画像情報、音声情報が適宜、含まれるデジタル文書Fの内、対象となる対象デジタル文書Gのダイジェストを作成するダイジェスト作成手段31と、このダイジェスト作成手段31で作成される複数のダイジェストを結合するダイジェスト結合手段33と、このダイジェスト結合手段33で複数のダイジェストを結合して得られた全体の結果に対して統合ダイジェストを作成する統合ダイジェスト作成手段35と、この統合ダイジェスト作成手段35で作成された統合ダイジェストを含むデータを時刻認証手段41を介してデジタル署名作成手段39に送付する送付手段37と、後述する時刻取得手段43aから取得した時刻を前記送付手段37を介して統合ダイジェスト作成手段35から受け取った統合ダイジェストを含むデータに結合し、この結合した全体に対してデジタル署名を作成するデジタル署名作成手段39と、これら各手段で作成され、取得された統合ダイジェスト、時刻、デジタル署名を含む時刻認証証明書を受取手段45に送付する時刻認証手段41と、この時刻認証手段41により問い合わせのあった時点の時刻を時刻情報として提供する時刻取得手段43aと、前記時刻認証手段41から送られる時刻認証証明書を受け取る受取手段45と、この受取手段45を介して受け取った時刻認証証明書の検証を行う検証手段47と、前記ダイジェスト作成手段31に対し、ダイジェストの作成タイミングを指示する時刻指定手段49と、デジタル文書Fから対象とするデジタル文書を指定するデジタル文書指定手段51と、前記ダイジェスト作成手段31、送付手段37、受取手段45および検証手段47に対し問い合わせのあった時点の時刻を時刻情報として提供する時刻取得手段43bにより構成される。なお、時刻取得手段43aと時刻取得手段43bは、同一であっても構わない。

【0039】ここで、ダイジェスト作成手段31と、ダイジェスト結合手段33と、統合ダイジェスト作成手段35と、送付手段37と、受取手段45と、検証手段47と、時刻指定手段49と、デジタル文書指定手段51と、時刻取得手段43bがクライアント部100を構成

し、デジタル署名作成手段39と時刻認証手段41と時刻取得手段43aがサーバ部200を構成する。

【0040】以下、図2を参照して、第二の実施形態における時刻認証処理について説明する。

【0041】パソコン上からアクセス可能なパソコン内部あるいはネットワーク上のテキスト、音声、画像、バイナリ情報あるいはそれらの組み合わせからなるデジタル文書Fに対して、デジタル文書指定手段51によりファイルまたはフォルダ単位で指定された対象デジタル文書Gを指定する。

【0042】ダイジェスト作成手段31が時刻取得手段43bから取得した時刻に基づき時刻指定手段49により指定された時刻になったことを検出したら、ダイジェスト作成手段31は対象デジタル文書Gに対して、各デジタル文書毎にSHA-1やMD5などのハッシュ関数を用いてダイジェストを作成する。

【0043】ハッシュ関数を h 、対象デジタル文書を g_1, g_2, \dots, g_n とすると、ダイジェスト作成手段31によりダイジェスト $h(g_1), h(g_2), \dots, h(g_n)$ が作成される。

【0044】ダイジェスト結合手段33により、例えば、ダイジェスト $h(g_1), h(g_2), \dots, h(g_n)$ を接続により結合した結果 $h(g_1) \cdot h(g_2) \dots h(g_n)$ を得る。結合結果から統合ダイジェスト作成手段35により統合ダイジェストを作成する。

【0045】統合ダイジェスト作成手段35で用いるハッシュ関数を i とすると、 $i(h(g_1) \cdot h(g_2) \dots h(g_n))$ が統合ダイジェストとなる。統合ダイジェスト $i(h(g_1) \cdot h(g_2) \dots h(g_n))$ を送付手段37により時刻認証手段41を介してデジタル署名作成手段39に送付する。

【0046】デジタル署名作成手段39は、統合ダイジェスト $i(h(g_1) \cdot h(g_2) \dots h(g_n))$ と時刻取得手段43aにより取得した時刻 t を含むデジタルデータに対して、デジタル署名 s を作成し、このデジタル署名 s を時刻認証手段41に送出する。

【0047】時刻認証手段41は、統合ダイジェスト $i(h(g_1) \cdot h(g_2) \dots h(g_n))$ 、時刻 t およびデジタル署名 s を含む時刻認証証明書を発行し受取手段45に送出する。

【0048】検証手段47は、受取手段45で受け取った時刻認証証明書についてデジタル署名がデジタル署名作成手段39で作成された正しいデジタル署名であることを検証する。

【0049】さらに、時刻認証証明書に付けられている時刻が送付手段37がデジタル署名作成手段39に送付した時刻以降であり、受取手段45が受け取った時刻以前であることを検証する。

【0050】上述したように、第二の実施形態によれ

ば、第一の実施形態における効果に加え、さらにフォルダあるいはファイル単位で指定したパソコン上のファイルに対して定期的に時刻認証証明書を取得し、パソコン上のファイルの作成変更履歴に関連するファイルとの関係を含めて記録することができ、また長い時間に渡って取得した時刻認証証明書の系列はパソコン上のファイルの作成変更履歴に対する第三者による証明書とすることができる。この時刻認証証明書の系列は、研究ノートや家計簿以上に偽造が難しいため、デジタル文書に対して信頼性の高い時刻認証手段の提供が可能となる。

【0051】なお、上述したこのようなフォルダ型時刻認証システム用のプログラムは記録媒体に記録して提供されることにより、該記録媒体を利用して、そのフォルダ型時刻認証プログラムの流通性を高めることができる。

【0052】次に、図3に本発明の第三の実施形態に係る分散時刻認証システムの構成を示す。

【0053】図3において、分散時刻認証システム101は、一定間隔を置いて少なくとも1回以上である n 回、各々独立にある一定の刻み幅の時刻情報 t_{1i}, \dots, t_{si} を取得する複数の時刻取得手段113a, 113b, \dots , 113sと、これら時刻取得手段113a, 113b, \dots , 113s毎に1つずつ設けられ、デジタル文書Mに時刻情報 t_{ij} を結合して、各々独立に時刻印付きデジタル文書 $M_{t_{ij}}$ を作成する、複数の結合手段111a, 111b, \dots , 111sと、これら結合手段111a, 111b, \dots , 111s毎に1つずつ設けられ、各々独立にデジタル署名を作成する複数のデジタル署名手段115a, 115b, \dots , 115sと、該複数のデジタル署名手段115a, 115b, \dots , 115sで独立に作成された複数のデジタル署名を受け取り、これら複数のデジタル署名の中から互いに等しい時刻印付きデジタル文書 M_t から作成されたデジタル署名を各デジタル署名手段115a, 115b, \dots , 115s毎に1つ選択し、それらの選択された互いに等しい時刻印付きデジタル文書 M_t に対して、作成されたデジタル署名から統合デジタル署名 c を作成する統合デジタル署名作成手段117と、これら時刻印付きデジタル文書 M_t および統合デジタル署名 c を含む時刻認証証明書Tを作成する時刻認証証明書作成手段119により構成される。

【0054】以下、図3を参照して第三の実施形態における分散時刻認証処理について説明する。ここでは結合手段111aの系を中心に説明を進めるが、他の系においても同様である。

【0055】著作者により作成されたテキスト文書、画像情報、音声情報、バイナリ情報あるいはそれらの組み合わせからなるデジタル文書Mから、分散時刻認証システム101内の結合手段111aにおいて、時刻取得手段113aにより取得された時刻と結合され時刻印付き

デジタル文書M_tが作成される。この作成された時刻印付きデジタル文書M_tに対するデジタル署名がデジタル署名手段115aにより作成される。このように各デジタル署名手段115a, 115b, …, 115sで作成されたデジタル署名は、統合デジタル署名作成手段117に集められる。

【0056】さらに統合デジタル署名作成手段117は、共通の時刻を持つ時刻印付きデジタル文書M_tがデジタル署名手段115毎に一つ選択することができる場合には、それらの共通の時刻を持つ時刻印付きデジタル文書M_tに対するデジタル署名から統合デジタル署名を作成する。続いて、時刻認証証明書作成手段119は、統合デジタル署名を作成するのに用いた時刻印付きデジタル文書M_tと統合デジタル署名を含む時刻認証証明書Tを作成する。

【0057】以下、デジタル署名作成について、一例をあげて説明する。なお、ここでは公開鍵暗号の具体例としてRSA公開鍵暗号を用いる。

【0058】まず、pとqを十分大きな素数とし、
 $n = p \cdot q$

とおく。そして、

$$\phi(n) = (p-1)(q-1)$$

と互いに素な整数eを適当に定める。すなわち、

$$\gcd(e, (p-1)(q-1)) = 1$$

そして、nとeを公開鍵とし、dを

$$ed = 1 \pmod{\phi(n)}$$

である整数とすると、p, q, dを秘密鍵とする。

【0059】共通の時刻を持つ時刻印付きデジタル文書M_tにハッシュ関数(例えばSHA-1やMD5)を適用して得られるダイジェストをmとする。

【0060】さらに、

$$c = m^d \pmod{n}$$

とおく。このとき、cを統合デジタル署名作成手段117により最終的に作成される統合デジタル署名とする。図3におけるデジタル署名手段115の総数をsとしたとき、dを数の和で表現して

$$d = d_1 + d_2 + \dots + d_s$$

とおく。

$$【0061】c_1 = m^{d_1} \pmod{n}, \dots,$$

$$c_s = m^{d_s} \pmod{n}$$

とすると、 c_1, \dots, c_s がs個のデジタル署名手段115a, 115b, …, 115sで作成されるデジタル署名となる。(M_t, c)を含むデジタル文書が時刻認証証明書Tとなる。

【0062】次に、図4に本発明の第四の実施形態に係る分散時刻認証システムの構成を示す。

【0063】図4において、分散時刻認証システム103は、デジタル文書Mを通信により受け取る受取手段130と、一定間隔を置いて少なくとも1回以上であるn回、各々独立にある一定の刻み幅の時刻情報 $t_{1i},$

…, t_{si} を取得する複数の時刻取得手段133a, 133b, …, 133sと、これら時刻取得手段133a, 133b, …, 133s毎に1つずつ設けられ、受取手段130で受けとったデジタル文書Mに時刻情報 t_{ij} を結合して、各々独立に時刻印付きデジタル文書M_{t_{ij}}を作成する複数の結合手段131a, 131b, …, 131sと、これら結合手段131a, 131b, …, 131s毎に1つずつ設けられ、各々独立にデジタル署名を作成する複数のデジタル署名手段135a, 135b, …, 135sと、これら複数のデジタル署名手段135a, 135b, …, 135sで独立に作成された複数のデジタル署名を受け取り、これら複数のデジタル署名の中から互いに等しい時刻印付きデジタル文書M_tから作成されたデジタル署名を各デジタル署名手段135a, 135b, …, 135s毎に1つ選択し、それらの選択された互いに等しい時刻印付きデジタル文書M_tに対して、作成されたデジタル署名から統合デジタル署名cを作成する統合デジタル署名作成手段137と、これら時刻印付きデジタル文書M_tおよび統合デジタル署名cを含む時刻認証証明書Tを作成する時刻認証証明書作成手段139と、この時刻認証証明書作成手段139で作成された時刻認証証明書Tを通信によりデジタル文書の送付者に返送する送付手段141により構成される。

【0064】図5および図6は、第三および第四の実施形態における取得時刻情報の関係を示す。ここでは、デジタル署名手段が3つある場合を例に取得時刻情報の関係を示している。図5および図6において、 t_{11}, t_{21}, t_{31} は、3つの時刻取得手段が1回目取得した時刻をそれぞれ表わし、 t_{12}, t_{22}, t_{32} は、3つの時刻取得手段が2回目取得した時刻をそれぞれ表わす。また、 t_{i1}, t_{i2}, t_{i3} は3つの時刻取得手段が第i回目に時刻取得を行ったときの正確な時刻をそれぞれ表し、 t_{j1}, t_{j2}, t_{j3} は3つの時刻取得手段が第j回目に時刻取得を行ったときの正確な時刻をそれぞれ表わす。

【0065】図5では、3つの時刻取得手段とも1回目に同じ時刻情報を取得し、2回目も同じ時刻情報を取得したことを表わす。この場合には、 $t_{11} = t_{21} = t_{31}$ が統合デジタル署名の作成に用いられる時刻となる。同様に、図6では、第一、第二の時刻取得手段の2回目と、第三の時刻取得手段の1回目が同じ時刻情報を取得したことを表わす。この場合には、 $t_{31} = t_{12} = t_{22}$ が統合デジタル署名の作成に用いられる時刻となる。

【0066】図7は、図6と比較して刻み幅を半分にした場合における時刻取得時の正確な時間と取得時刻情報の関係を示す。図7において、 t_{11}, t_{21}, t_{31} は、3つの時刻取得手段が1回目取得した時刻をそれぞれ表わし、 t_{12}, t_{22}, t_{32} は、3つの時刻取

得手段が2回目に取得した時刻をそれぞれ表し、 t_{13} 、 t_{23} 、 t_{33} は、3つの時刻取得手段が3回目に取得した時刻をそれぞれ表す。また、 t_{i1} 、 t_{i2} 、 t_{i3} は3つの時刻取得手段が第1回目に時刻取得を行ったときの正確な時刻をそれぞれ表し、 t_{j1} 、 t_{j2} 、 t_{j3} は3つの時刻取得手段が第2回目に時刻取得を行ったときの正確な時刻をそれぞれ表し、 t_{k1} 、 t_{k2} 、 t_{k3} は3つの時刻取得手段が第3回目に時刻取得を行ったときの正確な時刻をそれぞれ表す。この刻み幅を半分にした例では、3つの時刻取得手段により同じ時刻情報を取得するために、各時刻取得手段は少なくとも3回の時刻取得を行う必要がある。

【0067】なお、各時刻取得手段が時刻取得を行う一定間隔は、任意の長さに設定可能であるが、各時刻取得手段が取得する時刻の一定の刻み幅と等しく設定することが好ましい。

【0068】また、2回目以降の時刻取得を実際には行わずに、第1回目に取得した時刻に予め決められた一定の刻み幅の時間を順次加えて得られた時刻を2回目以降の取得時刻とすることも可能である。この場合には、各時刻取得手段は時刻取得を1回行うのみでよい。

【0069】各時刻取得手段が取得する時刻の一定の刻み幅は、任意の長さに設定可能であるが、刻み幅を小さくすればするほど、取得される時刻の精度が向上する反面、共通の時刻を持つ時刻印付きデジタル文書Mがデジタル署名手段毎に一つ選択できるようになるまで各デジタル署名手段が作成することになるデジタル署名の数は増えることになる。

【0070】但し、各結合手段にデジタル文書Mが到着する時間にばらつきがある場合には、以下のように、最も時間のかかる結合手段以外の結合手段に対応するデジタル署名手段において絶対に共通の時刻として使われることがない時刻の少なくとも一つに対するデジタル署名の作成は行わないようにして、デジタル署名の数を減らすことは可能である。

【0071】図8は、異なる2つの結合手段にデジタル文書が到着する可能性のある時間幅の関係を表している。図8の(1)は、一方の結合手段にデジタル文書が最も遅く到着し得る時刻より後にしかも一方の結合手段にデジタル文書が到着し得ない場合を表し、図8の

(2)は、一方の結合手段にデジタル文書が最も遅く到着し得る時刻が、もう一方の結合手段にデジタル文書が到着する可能性のある時間帯の中に含まれ、かつ、前者の結合手段にデジタル文書が最も早く到着し得る時刻が後者の結合手段にデジタル文書が最も早く到着し得る時刻よりも前になる場合を表し、図8の(3)は、一方の結合手段にデジタル文書が到着する可能性のある時間帯が、もう一方の結合手段にデジタル文書が到着し得る時間帯に完全に含まれる場合を表す。任意の2つの結合手段に同じデジタル文書が到着する時間帯の関係はこれら

3つのいずれかとなる。

【0072】図9は、最も遅くデジタル文書が到着する結合手段への到着時間帯が時刻cとdの間であり、それ以外の任意の結合手段にデジタル文書が到着する時間帯が時刻aとbの間である場合のa、b、c、dの前後関係を表す。図9の(1)、(2)、(3)はそれぞれ図8の(1)、(2)、(3)に相当するケースを示す。ここで最も遅くデジタル文書が到着する結合手段をC1、それ以外の任意の結合手段をC2とする。また、刻み幅すなわち t_i と t_{i+1} の間隔をuとする。

【0073】ここで、一般に、各結合手段は現在時刻以降の直近の予め決められた時刻に、統合デジタル署名作成に絶対使われることがない時刻を除くために予め指定された0以上の時間を加えて得られた時刻を開始時刻として、予め指定された時間間隔で得られる指定個数の時間を時刻情報としてデジタル文書に結合することにより時刻印付きデジタル文書を作成するものとすることが可能である。

【0074】ここで、予め指定された0以上の時間は、結合手段間でデジタル文書の到着時刻に固定的なずれがある場合に、本来は先に時刻印付きデジタル文書作成を開始する結合手段がそのずれに応じて時刻印付きデジタル文書作成の開始を遅らせるために使われる。

【0075】また、指定個数は、結合手段におけるデジタル文書の到着時刻の時間幅に変動がありえる場合にも、必ず統合デジタル署名を作ることができるようになるまでのデジタル署名手段に対しても共通する時刻の時刻印付きデジタル文書が求められるようにするために使われる。

【0076】図9の(1)の場合、 $(c-b)/u$ を超えない最大の整数値nとuとの積をvとし、時刻 t_3 と t_4 の間の時刻eにデジタル文書がC2に到着したとすると、現在時刻はeであり、 $n=1$ であるので、現在時刻以降の予め決められた時刻を t_4 、予め指定された0以上の時間は $v=n*u=1*u$ とすることが可能である。さらに、予め指定された時間間隔はuであり、指定個数は $(d-a)/u$ 以上の最小の整数値mに1を加えてからnを引いた数とすることが可能である。この場合には、 $m=5$ であるから、指定個数は $5+1-1=5$ となる。

【0077】この結果、 t_4 を時刻情報とする時刻印付きデジタル文書は作成する必要がなく、 t_4 にvを足して得られる t_5 からの指定個数5個の t_5 、 t_6 、 t_7 、 t_8 、 t_9 を時刻情報とする時刻印付きデジタル文書のみを作成すればよい。eがaと t_3 の間にある場合には、同様に t_4 、 t_5 、 t_6 、 t_7 、 t_8 を時刻情報とする時刻印付きデジタル文書のみを作成すればよい。eが t_4 とbの間にある場合には、同様に t_6 、 t_7 、 t_8 、 t_9 、 t_{10} を時刻情報とする時刻印付きデジタル文書のみを作成すればよい。

【0078】図9の(2)の場合、時刻 t_3 と t_4 の間の時刻 e にデジタル文書 C_2 に到着したとすると、現在時刻は e であり、現在時刻以降の予め決められた時刻を t_4 、予め指定された0以上の時間は0とすることが可能である。さらに、予め指定された時間間隔は u であり、指定個数は $(d-a)/u$ 以上の最小の整数値 m に1を加えた数とすることが可能である。この場合には指定個数は6となるので、 t_4 、 t_5 、 t_6 、 t_7 、 t_8 、 t_9 を時間情報とする時刻印付きデジタル文書のみを作成することになる。

【0079】図9の(3)の場合、時刻 t_5 と t_6 の間の時刻 e にデジタル文書 C_2 に到着したとすると、現在時刻は e であり、現在時刻以降の予め決められた時刻を t_6 、予め指定された0以上の時間は0とすることが可能である。さらに、予め指定された時間間隔は u であり、指定個数は $(d-a)/u$ 以上の最小の整数値 m に1を加えた数とすることが可能である。この場合には指定個数は3となるので、 t_6 、 t_7 、 t_8 を時間情報とする時刻付きデジタル文書のみを作成することになる。

【0080】さて、通常、分散時刻認証システムにあっては、構成要素のデジタル署名手段が公開鍵暗号における秘密鍵の一部を分散して保持するので、秘密鍵の盗難や時刻認証証明書の偽造の危険性を小さくすることができるものの、前述したように時刻取得手段が各々独立に取得した時刻が一致する可能性は非常に小さいため統合デジタル署名を作成できないという問題がある。

【0081】これに対し、第三、第四の実施形態では、上述してきたように、一定の刻み幅で時刻を取得するので、各々独立に取得した時刻が等しくなる可能性を高くできる。実際、図5および図6に示した例においては、一定間隔において最低2回の時刻取得を各時刻取得手段毎に行えば、刻み幅と時刻取得手段間の時刻取得実行時間差の関係から必ず共通する時刻印付きデジタル文書をすべての結合手段で得ることが可能となる。この結果、秘密鍵の安全性を向上させる分散時刻署名が可能となる。

【0082】このような分散時刻認証プログラムは記録媒体に記録して提供されることにより当該分散時刻認証プログラムの流通性を高めることができる。

【0083】なお、上述した第三、第四の実施形態では、RSAを公開鍵暗号に用いた場合について説明したが、本発明はこれに限定されることなく楕円曲線公開鍵暗号、DSA (Digital Signature Algorithm) 等の秘密鍵を分割し、単一の秘密鍵で作成するデジタル署名と同じデジタル署名を、複数の分割した秘密鍵から作成することが可能な公開鍵暗号を用いても同様にデジタル署名および統合デジタル署名を作成することが可能である。

【0084】また、時刻印付きデジタル文書 M_t の代わりに時刻印付きデジタル文書 M を含むデジタル文書を

用いて統合デジタル署名を作成しても、何ら問題はない。さらにデジタル文書にハッシュ関数を適用せずに直接デジタル署名を作成することも可能である。また、1つの時刻印付きデジタル文書 M_t に1つの時刻情報を対応させるものであっても、1つの時刻印付きデジタル文書 M_t に複数の時刻情報を対応させるものであっても良い。つまり1つの時刻情報に対応する場合には1つの時刻印付きデジタル文書 M_t から1つのデジタル署名が作成され、複数の時刻情報に対応する場合には1つの時刻印付きデジタル文書 M_t から複数のデジタル署名が作成されることになる。

【0085】次に、図10に本発明の第五の実施形態に係るフォルダ型分散時刻認証システムの構成を示す。この第五の実施形態は、上述した第一および第二の実施形態と、第三および第四の実施形態とを組み合わせたものである。

【0086】図10において、フォルダ型分散時刻認証システム300は、クライアント部100とサーバ部200からなる。クライアント部100は時刻認証対象である複数のデジタル文書 G から時刻認証要求 R を作成し、サーバ部200に渡す。サーバ部200は、受け取った時刻認証要求 R に基いて時刻認証証明書 T を作成し、クライアント部100に返す。

【0087】図11に、図10のフォルダ型分散時刻認証システム300におけるクライアント部100の構成例を示す。図11のクライアント部100は、上述した第二の実施形態における図2のクライアント部100に相当するものであり、同一構成要素には同一符号を付してある。

【0088】まず、デジタル文書指定手段51により、デジタル文書の集合 F のなかから時刻認証の対象となるデジタル文書 G を選択する。

【0089】次に、時刻指定手段49が指定する定期的なダイジェスト作成時刻において、ダイジェスト作成手段31により、選択されたデジタル文書毎にダイジェストを作成する。ここで前回ダイジェストを作成した後で内容に変更がないデジタル文書については前回作成したダイジェストを利用することも可能である。

【0090】次に、ダイジェスト結合手段33により、対象デジタル文書 G のそれぞれについてダイジェスト作成手段31が作成したダイジェストを結合して一つの新たなデジタル文書を作成する。

【0091】次に、統合ダイジェスト作成手段36により、この新たなデジタル文書から統合ダイジェストを作成する。

【0092】そして、統合ダイジェストを含む時刻認証要求 R を送付手段37からサーバ部200に送付する。

【0093】サーバ部200では、後述するように時刻認証証明書 T を作成し、クライアント部100の受取手段45に送付する。

【0094】次に、検証手段47が、送付手段37による送付時刻と、受取手段45による受取時刻と、受け取った時刻認証証明書Tに記録されている認証時刻を比較し、更に時刻認証証明書Tに含まれるデジタル署名がサーバ部200により作成された真正なデジタル署名であることを、サーバ部200が用いた秘密鍵に対応する公開鍵を用いて検証し、更に時刻認証証明書Tで時刻認証されているダイジェストが送付手段37により送付されたものであるかどうか検証する。

【0095】ここで、対象デジタル文書Gに前回の時刻認証証明書を含めることにより、対象デジタル文書Gの過去の作成、変更履歴を含めた時刻認証証明書を取得することが可能となる。

【0096】図12に、図10のフォルダ型分散時刻認証システム300におけるサーバ部200の一構成例を示す。図12のサーバ部200は、上述した第四の実施形態における図4の分散時刻認証システムに相当するものであり、同一構成要素には同一符号を付してある。

【0097】まず、受取手段130が時刻認証要求Rを受け取ると、そのコピーを各結合手段131に送る。

【0098】次に、各結合手段131は、該当する時刻取得手段133により取得された時刻と時刻認証要求Rに含まれるデジタル文書Mを結合して時刻印付きデジタル文書Mtを作成する。

【0099】次に、この作成された時刻印付きデジタル文書Mtに対するデジタル署名を、該当するデジタル署名手段135において予め取得している部分秘密鍵により作成する。このように各デジタル署名手段135で作成されたデジタル署名は、統合デジタル署名作成手段137に集められる。

【0100】次に、統合デジタル署名作成手段137は、集められたデジタル署名のなかから、共通の時刻情報を持つデジタル署名を各デジタル署名手段135毎に一つ選択し、統合デジタル署名を作成する。

【0101】そして、時刻認証証明書作成手段139が、作成された統合デジタル署名を用いて時刻認証証明書Tを作成し、これを送付手段141からクライアント部100に送付する。

【0102】図13に、図10のフォルダ型分散時刻認証システム300におけるサーバ部200の他の構成例を示す。図13は、サーバ部200の機能を独立した第三者機関により運用する分散配置構成を示すものであり、上述した図12のサーバ部200と同一構成要素には同一符号を付してある。

【0103】図13においては、結合手段131、時刻取得手段133、デジタル署名手段135各一つずつの一组が一つの分散部分時刻認証機関205を構成し、受取手段130、統合デジタル署名作成手段137、時刻認証証明書作成手段139、送付手段141が一つの時刻認証機関204を構成している点が図12と異なる

が、各手段の動作は図12の場合と同じである。

【0104】

【発明の効果】上述したように、本発明のフォルダ型時刻認証システムによれば、パソコン上のデジタル文書に対して定期的に信頼のおける第三者機関から存在証明のための時刻認証証明書を取得しておくことにより日常的に履歴の残る記録とし、かつ変更作成記録を第三者に証明することが可能となる。

【0105】また、本発明の分散時刻認証システムによれば、必ず共通する時刻印付きデジタル文書をすべての結合手段で得ることが可能となるので、秘密鍵の安全性を向上させる分散時刻署名が可能となる。

【図面の簡単な説明】

【図1】本発明の第一の実施形態におけるフォルダ型時刻認証システムの構成例を示すブロック図。

【図2】本発明の第二の実施形態におけるフォルダ型時刻認証システムの構成例を示すブロック図。

【図3】本発明の第三の実施形態における分散時刻認証システムの構成例を示すブロック図。

【図4】本発明の第四の実施形態における分散時刻認証システムの構成例を示すブロック図。

【図5】図3および図4の分散時刻認証システムにおいて取得される取得時刻情報の一例を示す図。

【図6】図3および図4の分散時刻認証システムにおいて取得される取得時刻情報の他の例を示す図。

【図7】図3および図4の分散時刻認証システムにおいて取得される取得時刻情報の他の例を示す図。

【図8】図3および図4の分散時刻認証システムにおいて異なる2つの結合手段にデジタル文書が到着する可能性のある時間幅の関係を示す図。

【図9】図3および図4の分散時刻認証システムにおいて異なる2つの結合手段にデジタル文書が到着する可能性のある時間幅と到着時刻の例を示す図。

【図10】本発明の第五の実施形態におけるフォルダ型分散時刻認証システムの構成例を示すブロック図。

【図11】図10のフォルダ型分散時刻認証システムにおけるクライアント部の一構成例を示すブロック図。

【図12】図10のフォルダ型分散時刻認証システムにおけるサーバ部の一構成例を示すブロック図。

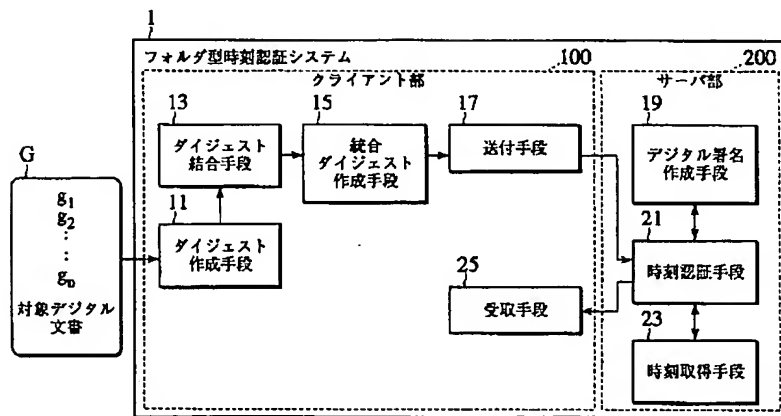
【図13】図10のフォルダ型分散時刻認証システムにおけるサーバ部の他の構成例を示すブロック図。

【符号の説明】

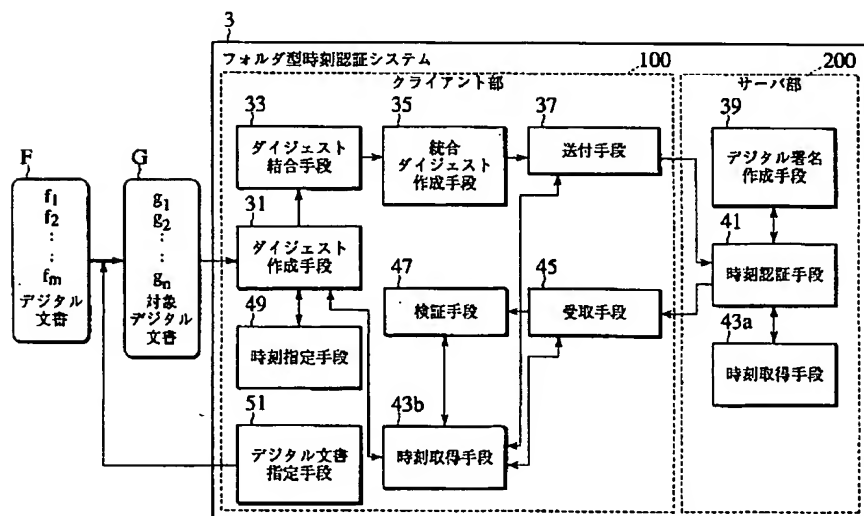
- 1, 3 フォルダ型時刻認証システム
- 11, 31 ダイジェスト作成手段
- 13, 33 ダイジェスト結合手段
- 15, 35 統合ダイジェスト作成手段
- 17, 37 送付手段
- 19, 39 デジタル署名作成手段
- 21, 41 時刻認証手段
- 23, 43 時刻取得手段

- | | |
|---------------------|-----------------------|
| 25, 45 受取手段 | 117, 137 統合デジタル署名作成手段 |
| 47 検証手段 | 119, 139 時刻認証証明書作成手段 |
| 49 時刻指定手段 | 130 受取手段 |
| 51 デジタル文書指定手段 | 141 送付手段 |
| 100 クライアント部 | 200 サーバ部 |
| 101, 103 分散時刻認証システム | 300 フォルダ型分散時刻認証システム |
| 111, 131 結合手段 | M デジタル文書 |
| 113, 133 時刻取得手段 | T 時刻認証証明書 |
| 115, 135 デジタル署名手段 | R 時刻認証要求 |

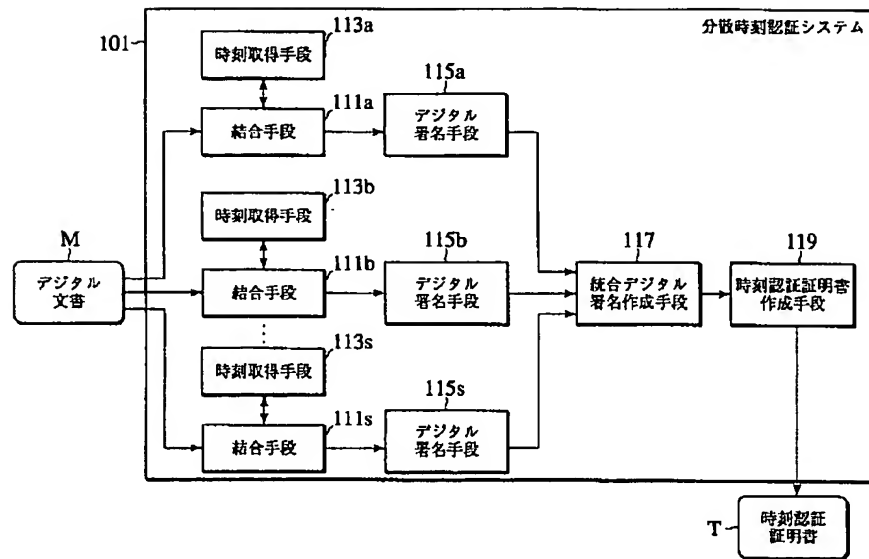
【図1】



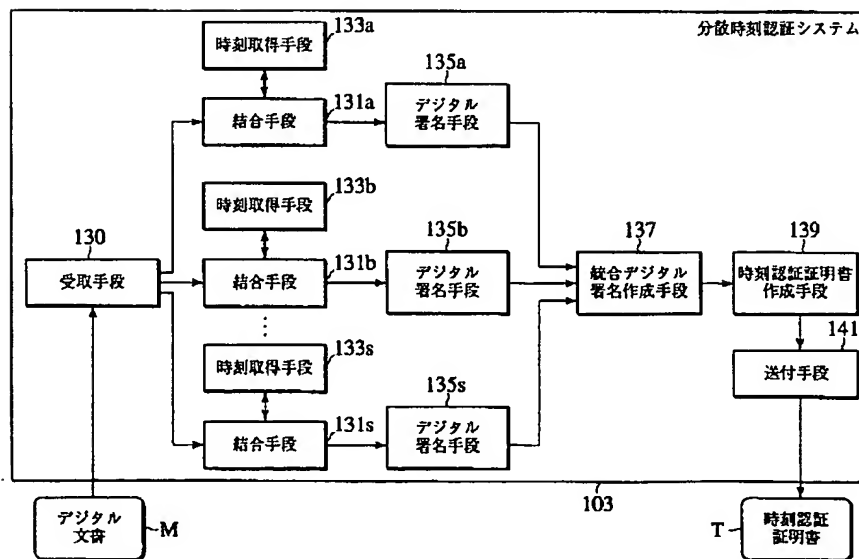
【図2】



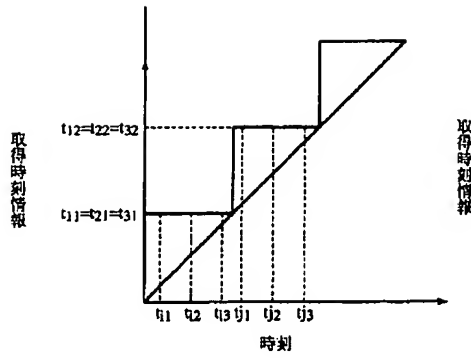
【図3】



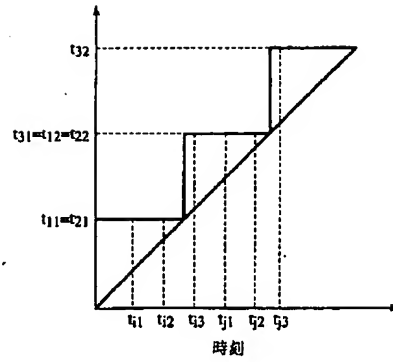
【図4】



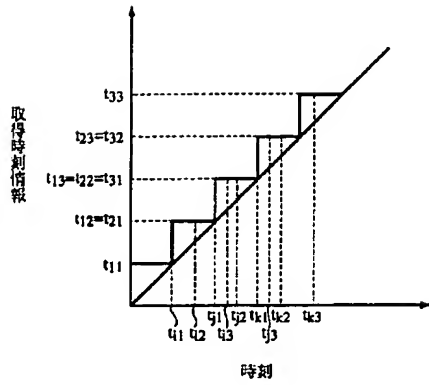
【図5】



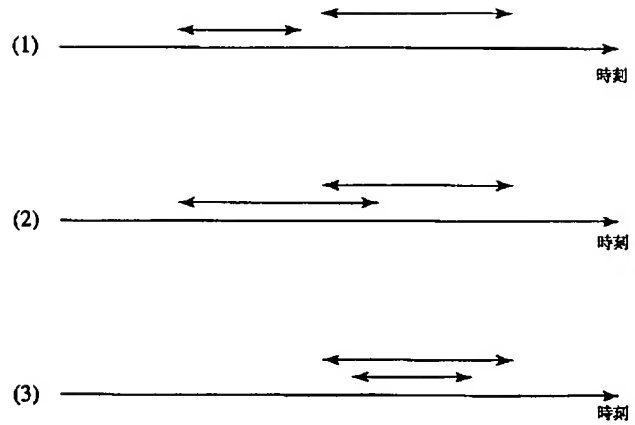
【図6】



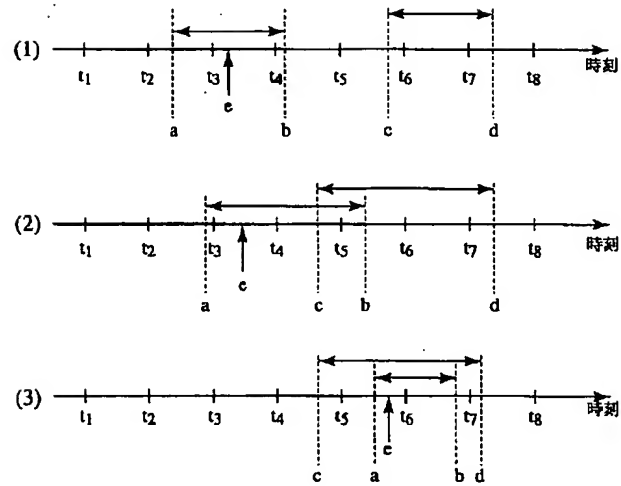
【図7】



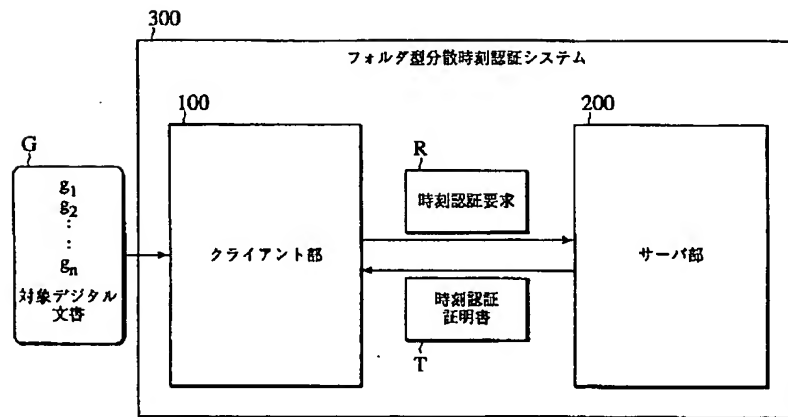
【図8】



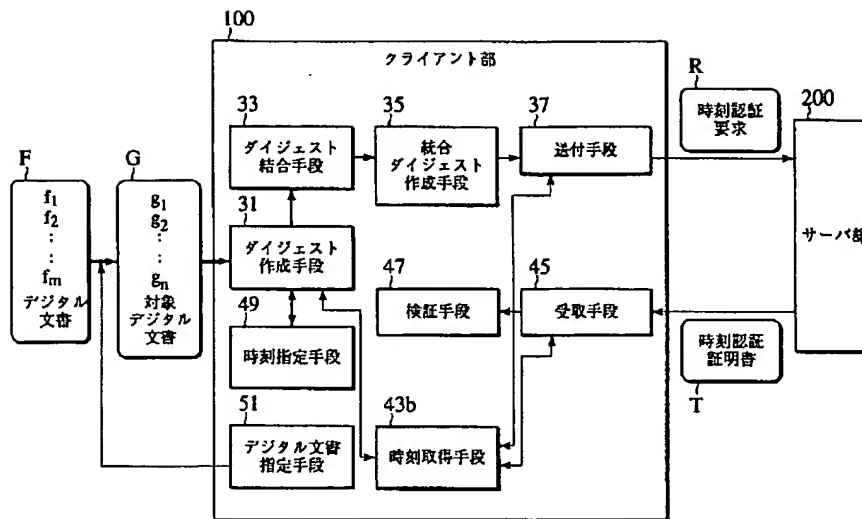
【図9】



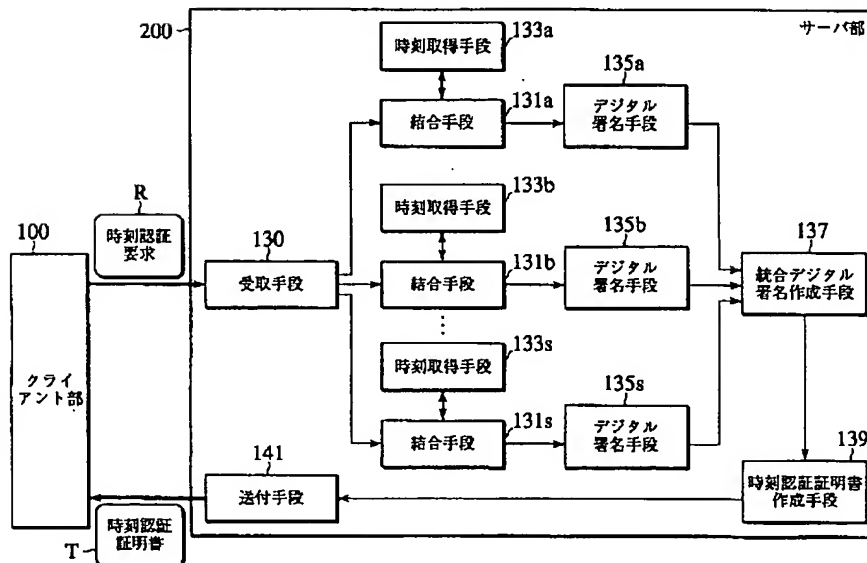
【図10】



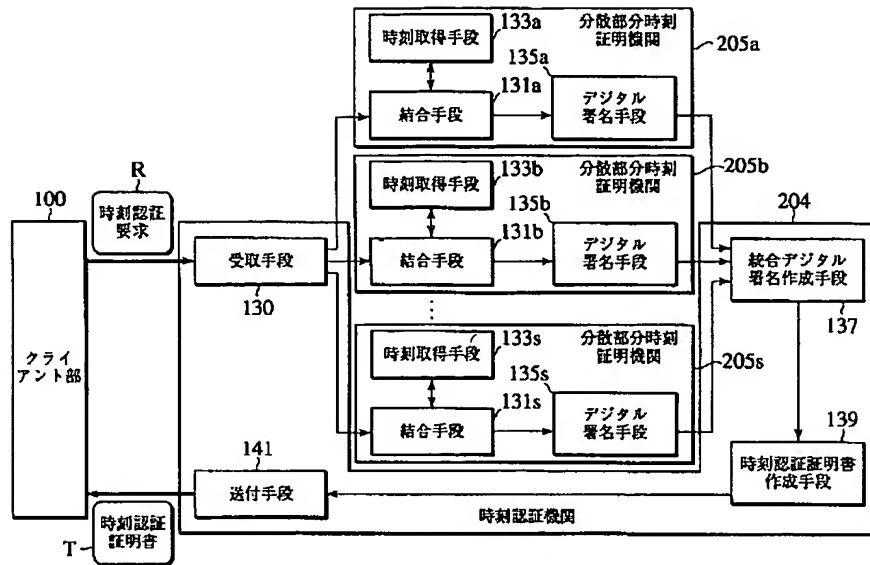
【図11】



【図12】



【図13】



POWERED BY **Dialog**

FOLDER TYPE TIME CERTIFYING SYSTEM AND DISTRIBUTED TIME CERTIFYING SYSTEM**Publication Number:** 2001-142398 (JP 2001142398 A) , May 25, 2001**Inventors:**

- TAKURA AKIRA
- ONO SATOSHI

Applicants

- NIPPON TELEGR & TELEPH CORP (NTT)

Application Number: 2000-266194 (JP 2000266194) , September 01, 2000**Priority:**

- 11-247993 [JP 99247993], JP (Japan), September 01, 1999
- 11-247994 [JP 99247994], JP (Japan), September 01, 1999

International Class:

- G09C-001/00

Abstract:

PROBLEM TO BE SOLVED: To provide a time certification system for making a digital document on a personal computer a record holding a daily history and for certifying a change and preparation record to a third party.

SOLUTION: In this time certification system, a client device prepares a plurality of digests of a plurality of digital documents, combines the prepared digests, prepares an integrated digest from the combined digests, sends a time certification request including the prepared integrated digest to a server device and receives a time certification with respect to the digital documents from the server. The server device prepares the time certification including the digital document with a time work obtained by combining time information obtained in response to the time certification request and the integrated digest and a digital signature to the digital document with the time mark. COPYRIGHT: (C) 2001,JPO

JAPIO

© 2004 Japan Patent Information Organization. All rights reserved.

Dialog® File Number 347 Accession Number 6914862

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.